Relatório de Auditoria Interna de Rede Doméstica

Autor: George de Moura Marques Nóbrega
Objetivo: Realizar auditoria interna em rede doméstica com foco educacional e de segurança cibernética.
Escopo: Todos os dispositivos conectados à rede local. Endereços IP foram mascarados (10.0.0.x).

1. Metodologia Utilizada

Foram empregados métodos de auditoria passiva e ativa utilizando principalmente a ferramenta Nmap:
• Descoberta de hosts (Nmap -sn)
• Enumeração de portas TCP (Nmap -sV, -sC, -p-)
• Enumeração de portas UDP (Nmap -sU --top-ports 30)
• Detecção de serviços e SO (Nmap -O)
• Auditoria sem exploração, seguindo boas práticas éticas

2. Resultados da Auditoria

Roteador (10.0.0.1 e 10.0.0.2):
Serviços internos do firmware (SNMP, ISAKMP, SYSLOG), porém sem acessos permitidos via LAN. Nenhuma vulnerabilidade explorável detectada.

Notebook Windows (10.0.0.9):
Dispositivo completamente blindado. Nenhuma porta TCP ou UDP aberta. Firewall ativo e efetivo, configurado no perfil privado/público.

VM Kali Linux (10.0.0.5):
Host identificado como ambiente controlado. Sem riscos significativos.

Dispositivos Android/iPhone (10.0.0.3 / 10.0.0.4 / 10.0.0.8):
Nenhuma porta visível. Android com MAC aleatório e firewall integrado ativo. ADB não exposto. iPhone com postura altamente restritiva.

TV LG (10.0.0.x):
Nenhuma porta TCP/UDP aberta durante análise. Firewall interno da TV ativo.

3. Conclusão Geral

A rede doméstica apresenta excelente postura de segurança. Nenhum dispositivo analisado expôs serviços sensíveis ou portas abertas que pudessem representar risco. O roteador permanece com serviços internos habilitados, mas isolados para uso exclusivo do firmware, não respondendo a tentativas externas via LAN.

A auditoria demonstra corretamente o uso de técnicas de pentest defensivo, conhecimento de ferramentas e respeito aos limites éticos.

4. Recomendações de Melhoria

• Manter firewalls ativos em todos os dispositivos

- Evitar ativar ADB em celulares
- Atualizar regularmente o firmware do roteador
- Criar rede separada para dispositivos IoT, se possível
- Usar VMs vulneráveis (DVWA, Metasploitable) para testes reais e seguros