



PORT SCANNING ATTACK

Filipe da Rosa Fiti¹

Anderson santos da silva²

Mario Oscar Steffen³

Luis Orlandro Chamorro Vergara⁴

RESUMO

Prática muito usada em qualquer tipo de rede, seja ele empresarial, domiciliar ou até pública, a abertura de portas para execução correta de uma aplicação, é uma prática que se não for aplicada corretamente pode trazer sérios problemas por isso a orientação que sempre temos é de manter as portas fechadas exceto se você tiver noção do que está fazendo.

Palavras-chave: Port scaningng attack.

ABSTRACT

A practice widely used in any type of network, be it business, home or even public, the opening of doors for the correct execution of an application is a practice that, if not applied correctly, can bring serious problems, so the guidance we always have is to keep the doors closed unless you know what you're doing.

Keywords: port scaningng attack.

¹ Aluno da Faculdade Alcides Maya - guilherme.hubner@alcidesmaya.edu.br

² Professor da Faculdade Alcides Maya – anderson_silva@alcidesmaya.edu.br

³ Professor da Faculdade Alcides Maya – mario_steffen@alcidesmaya.edu.br

⁴ Professor da Faculdade Alcides Maya – luis_chamorro@alcidesmaya.edu.br



A falta de conhecimento atinge uma grande parcela de empresas seja elas por falta de investimentos e a técnicos por falta de estudos para defender suas redes de ataques em portas de roteadores. Ainda que um técnico tenha noção de uma correta liberação de porta em um roteador, deve se levar em conta as falhas de segurança que ele irá expor com base na aplicação a qual está sendo liberada para a rede externa. A título de exemplo, um usuário que ainda rode Linux 2.3 que não possui mais atualizações, possui pelo menos 65 brechas de segurança. Usar esse sistema seria uma opção segura?

De acordo com uma pesquisa realizada pela cybersecurity-insiders, as portas mais suscetíveis a ataques em 2019 foram as portas 22 (ssh), 80 (http) e 443 (https). A Terceira e quarta porta mais vulneráveis foram as de serviço RDP serviço de acesso remoto (Microsoft) e FTP. Na grande maioria configurada com impressoras de médio porte, câmeras e nobreaks.

Uma das Ferramentas mais utilizadas para o escaneamento de porta é a ferramenta NMAP. O NMAP mapeia toda a rede atrás de portas que estejam abertas, gerando um relatório de serviços da rede alvo, iniciando assim um possível caminho para análise de um ataque. Uma vez detectada uma porta aberta, se inicia uma busca por brecha através do serviço detectado, o sucesso desse ataque vai depender do conjunto de sistemas que roda através do serviço. Se você é administrador de uma rede ao qual você externa serviços como website, leve em conta manter sempre sistema, firewall, plataforma do website seja ele em joomla, wordpress etc, com suas atualizações em dia. Proteja sua rede!

Essas são algumas das ferramentas de port scanning: NMAP, Advanced Port scanner, gwebtools



REFERÊNCIAS

NAVEN GOUD. 2020. **THESE THREE TCP PORTS ARE VULNERABLE TO CYBER ATTACKS**. DISPONÍVEL EM: <[HTTPS://WWW.CYBERSECURITY-INSIDERS.COM/THESE-THREE-TCP-PORTS-ARE-VULNERABLE-TO-CYBER-ATTACKS/](https://www.cybersecurity-insiders.com/these-three-tcp-ports-are-vulnerable-to-cyber-attacks/)>. ACESSO EM: 24 DE OUTUBRO DE 2020.

Wikipedia. **Port scanner**. 2020. Disponível em: <https://en.wikipedia.org/wiki/Port_scanner>. Acesso em 24 de Outubro de 2020.