Redes de Computadores II – NMAP

Daniel Veiga da Silva Antunes

NMAP (Network Mapper) trata-se de uma ferramenta muito poderosa, de código aberto, para mapeamento de rede, capaz de verificar máquinas pelas portas UDP e TCP, analisar a segurança de computadores, descobrir falhas em serviços, servidores ou rede de computadores.

Na modalidade padrão o NMAP utiliza pacotes SYN para a descoberta das portas TCP abertas. Enviando um pacote SYN e aguardando a resposta SYN + ACK e depois é enviando um ACK, fazendo a conexão inteira utilizado as 3 fazes da conexão de 3 vias.

Quando é enviado um SYN e obtém resposta que dá continuidade a conexão, a ferramenta identifica que a porta está aberta. Quando recebe um RST, identifica que a porta está fechada. Pois em ambientes normais um host iria responder com RST quando houver uma solicitação a uma porta que está fechada. Porém, podemos ter um firewall filtrando as respostas e assim, ao invés de responder com um RST, o host descarta o pedido de conexão. Quando isso ocorre a ferramenta informa que a porta está filtrada.