INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

SEGURANÇA DE REDES

ATIVIDADE 3 – NMAP / Wireshark / Tcpdump

Nome: _____

PARTE 1 – Conhecer as características e funcionalidades do nmap, acompanhando a ação do programa através de um analizador de protocolos (Utilize o wireshark/tcpdump)

1. Verifique na man page do nmap as opções de operação.

2. Faça um scan em sua própria máquina utilizando a opção padrão (sem opções).

3. Utilize o modo verbose do nmap e acompanhe o comportamento no analisador de protocolos.

4. Teste outros modos de *scan* do namap. Teste os modos *stealth* e acompanhe o andamento da varredura no wireshark/tcpdump. Procure entender o que está acontecendo e comprovar os conceitos do material didático.

5. Explore a capacidade do namp realizar verificação de OS Fingerprint. Realize essa tarefa nos servidores indicados pelo professor.

PARTE 2 – Exercício realizado em grupo, com objetivo de reconhecer ataque em andamento em sua rede. As ferramentas tcpdump/wireshark são simples, mas bastante poderosas, capazes de identificar uma série de comportamentos anormais em uma rede.

1. Peça ao colega para realizar um ataque utilizando a técnica de *Connect Scan*. Capture os pacotes com o Wireshark/tcpdump, analise e identifique o ataque em andamento. Tente explicar os motivos de sua conclusão.

2. Agora você deverá executar um ataque integrando FIN Scan e Null Scan. Capture os pacotes com o Wireshark/tcpdump, analise e identifique o ataque em andamento. Tente explicar os motivos de sua conclusão.

3. Realize um ataque em modo *Decoy* na máquina de seu companheiro de grupo. Capture os pacotes com o Wireshark/tcpdump, analise e identifique o ataque em andamento. Tente explicar os motivos de sua conclusão.