Segurança
Experimento N°01
Portscan com NMAP e Wireshark

Disciplina	**Segurança em Redes de Computadores**
Professor:	**Rafael Timóteo de Sousa Júnior**
Monitores:	**Valério Martins (valerioaymoremartins@gmail.com)** **Mariana Stieljes**

1. Introdução:

O NMAP é uma ferramenta de código aberto, utilizada para exploração de rede e auditoria de segurança. Ela foi desenvolvida para identificar as portas de serviço que estão abertas na máquina-alvo ou em um conjunto de máquinas.

O objetivo deste experimento é utilizar a ferramenta NMAP para avaliar a segurança da rede e identificar os ativos de rede, serviços e sistemas operacionais existentes na rede. Este objetivo suporta o estudo das técnicas de "*Information Gathering*".

2. Ambiente e Necessidades Preliminares

- Será utilizada a instalação existente do nmap no LInux Kali. Adicionalmente códigos-fontes em python serão disponibilizados.
- Não se esqueça de identificar seu IP no início do experimento.
- É importante que o aluno tenha conhecimento do uso do wireshark em "modo promíscuo".
- O Wireshark sempre deve ser ativado ao início e cada experimento. Ao final de cada atividade do experimento, leve ou encaminhe por email o arquivo de resultado.
- É importante que o aluno tenha conhecimento de como usar o redirecionador ">" em comandos do SO Linux para gerar arquivos textuais com os resultados de cada chamada do experimento.
- Sempre que for executar um comando em linha utilize o "sudo" antecipadamente
- No ambiente de host da VM pedimos desligar o firewall do Windows antes de abrir a VM e, antes de sair, liga-lo novamente.
- Lembre-se que você pode construir seu experimento usando comandos do Python. Ex.: files = os.popen("nmap ...").

3. **Atividades de Preparação (conhecimento inicial):**
   - Scan em um único endereço

     sudo nmap 172.16.5.1

     sudo nmap -v 172.16.5.1
   - Scan em um host pelo nome

     sudo nmap <nome_do_host>
   - Scan em um host pelo nome e obtendo mais informações

     sudo nmap -v <nome_do_host>
   - Scan múltiplos endereços ou sub-redes (IPv4)

     sudo nmap 172.16.5.1 172.16.5.2 172.16.5.3
   - Scan de um grupo na sub-rede 172.16.5.0/24

     sudo nmap 172.16.5.1,2,3

     sudo nmap 172.16.5.1-20
   - Scan em uma sub-rede inteira (CIDR e caracter curinga):

     sudo nmap 172.16.5.*

     sudo nmap 172.16.5.0/24
   - Lendo uma lista de redes ou hosts em um arquivo (IPv4)

     sudo nmap -iL /tmp/test.txt
   - Excluindo hosts ou sub-redes (IPv4)

     sudo nmap 172.16.5.0/24 --exclude 172.16.5.5

     sudo nmap 172.16.5.0/24 --exclude 172.16.5.5,172.16.5.254
   - Detectando a versão do sistema operacional (IPv4)

     sudo nmap -A 172.16.5.254

     sudo nmap -v -A 172.16.5.1

     sudo nmap -A -iL /tmp/scanlist.txt

- Descoberta se o alvo é protegido por um firewall

  sudo nmap -sA 172.16.5.254

  sudo nmap -sA <nome_do_host>
- Scan quando o host é protegido por um firewall

  sudo nmap -PN 172.16.5.1

  sudo nmap -PN <nome_do_host>
- Scan para descobrir quais servidores e dispositivos estão funcionando

  sudo nmap -sP 172.16.5.0/24

  sudo nmap -sP 172.16.5.1/24
- Geração de arquivos textuais de saída

  sudo nmap -sP -oA -n 172.16.5.1/24 <arquivo_scan>
- Executando uma verificação rápida

  sudo nmap -F 172.16.5.1
- Mostrando a razão da porta estar em determinado estado

  sudo nmap --reason 172.16.5.1

  sudo nmap --reason <nome_do_host>
- Mostrando apenas portas abertas (ou possivelmente abertas)

  sudo nmap --open 172.16.5.1

  sudo nmap --open <nome_do_host>
- Mostrando todos os pacotes enviados e recebidos

  sudo nmap --packet-trace 172.16.5.1

  sudo nmap --packet-trace <nome_do_host>
- Mostrando interface e rotas dos hosts

  sudo nmap --iflist

- Especificando uma porta (map -p [port] hostName)

  sudo nmap -p 80 172.16.5.1

  sudo nmap -p T:80 172.16.5.1

  sudo nmap -p U:53 172.16.5.1

  sudo nmap -p 80,443 172.16.5.1

  sudo nmap -p 80-200 172.16.5.1

  sudo nmap -p U:53,111,137,T:21-25,80,139,8080 172.16.5.1

  sudo nmap -p U:53,111,137,T:21-25,80,139,8080 <nome_do_host>

  sudo nmap -v -sU -sT -p U:53,111,137,T:21-25,80,8000 172.16.5.254

  sudo nmap -p "*" 172.16.5.1

  sudo nmap --top-ports 5 172.16.5.1

  sudo nmap --top-ports 10 172.16.5.1

- Maneira mais rápida de descobrir todas as portas e computadores em uma rede

  sudo nmap -T5 172.16.5.0/24

- Detectando um sistema operacional remoto

  sudo nmap -O 172.16.5.1

  sudo nmap -O 172.16.5.1

  sudo nmap -O --osscan-guess 172.16.5.1

  sudo nmap -v -O --osscan-guess 172.16.5.1

- Detectando serviços remotos e sua versão

  sudo nmap -sV 172.16.5.1

  sudo nmap -sV 172.16.5.1/24

  sudo nmap -sV 172.16.5.197

- Scan de host usando TCP ACK (PA) e TCP Syn (PS) ping

  sudo nmap -PS 172.16.5.1

sudo nmap -PS 80,21,443 172.16.5.1

sudo nmap -PA 172.16.5.1

sudo nmap -PA 80,21,200-512 172.16.5.1

- Scan em host usando ping

  sudo nmap -PO 172.16.5.1

- Scan a host usando UDP ping

  sudo nmap -PU 172.16.5.1

  sudo nmap -PU 2000.2001 172.16.5.1

- Portas mais utilizadas usando TCP SYN

  sudo nmap -sS 172.16.5.1

  sudo nmap -sS 172.16.5.1 -p 80

- Portas mais utilizadas utilizando TCP connect

  sudo nmap -sT 172.16.5.1

- Portas mais usadas utilizando TCP ACK
  sudo nmap -sA 172.16.5.1
- Portas mais usadas utilizando TCP window

  sudo nmap -sW 172.16.5.1

- Portas mais usadas utilizando TCP Maimon

  sudo nmap -sM 172.16.5.1

- Scan de host utilizando serviços UDP (UDP scan)

  sudo nmap -sU nas03

  sudo nmap -sU 172.16.5.1

- Scan pelo protocolo IP

  sudo nmap -sO 172.16.5.1

4. Experimento

O objetivo deste experimento é entender o funcionamento do NMAP.

A partir do acesso a linha de comando do ambiente da VM, faça as seguintes varreduras (não se esqueça de ativar o wireshark):

a) Ative em uma linha de comando separada um servidor HTTP no Python de sua máquina. Lembrar que ele vai entrar por default na porta 8000. Ex.: **python3 -m http.server**

b) Faça a varredura do seu IP, do IP seguinte ativo e do servidor informado em sala de aula (com a respectiva varredura de portas) da sala de aula. Antecipe e otimize usando os comandos apresentados no tópico "Atividades de preparação" (tal como testar apenas as portas 21 a 443, e adicionalmente a 8000). Sugerimos realizar processos de scan "controlados", indo da descoberta "do que existe" como IPs e as portas somente desse IP, e uma varredura mais profunda específica desses pares IP:porta.

c) Faça uma varredura das máquinas acima tentando observar o Sistema Operacional.

d) Faça a varredura direcionado a portas específicas (TCP e UDP: -p T:xxx,xxx U:xxx,xxx) usando sua máquina na lista.

e) Analise uma porta TCP (do seu IP e do IP indicado em sala de aula) usando os parâmetros -sS, -sT, -sA,

f) Coloque no ar um serviço UDP na sua máquina e analise esse serviço UDP (do seu IP) usando o parâmetros -sU. Analise também o da máquina indicada na sala de aula.

Obs.:

1) No tópico de "Desenvolvimento Teórico" do trabalho explique os pacotes TCP e UDP e seus flags / situações de ativação.

2) IP indicado em sala de aula (servidor na blade): 172.16.5.18.