Nmap

O **Nmap** (“Network Mapper”) é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. O **Nmap** utiliza pacotes IP em estado bruto (raw) de maneira inovadora para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts oferecem, quais sistemas operacionais (e versões de SO) eles estão executando, que tipos de filtro de pacotes/firewalls estão em uso, e dezenas de outras características. Embora o Nmap seja normalmente utilizado para auditorias de segurança, muitos administradores de sistemas e rede consideram-no útil para tarefas rotineiras tais como inventário de rede, gerenciamento de serviços de atualização agendados, e monitoramento de host ou disponibilidade de serviço.

Manual do Nmap em Português:
http://nmap.org/man/pt_BR/index.html#man-description

Planilha de comandos: http://remote-execution.blogspot.com/search/label/Nmap

1) Obter a lista de servidores com uma porta aberta específica

nmap -sT -p 80 -oG – 192.168.1.* | grep open

Alterar o argumento -p para o número da porta. Consulte “man nmap” para ver maneiras diferentes para especificar faixas de endereços

2) Fazer ping em um intervalo de endereços IP

nmap -sP 192.168.1.100-254

nmap aceita uma grande variedade de addressing, multiplos targets/ranges, etc…

3) Obter informações sobre as portas de host remoto e detecção de SO

nmap -sS -P0 -sV -O

Onde pode ser um único IP, um nome ou uma sub-rede

-sS TCP SYN scanning (também conhecido como half-open(semi-aberto) ou stealth scanning)

-P0 permite que você desligue pings ICMP.

-sV permite a detecção da versão

-O flag que permite a tentativa de identificar o sistema operacional remoto

Outras opções:

-A opção permite que ambos OS fingerprinting e detecção de versão

-v use **-vv** duas vezes para obter mais detalhamento.

nmap -sS -P0 -A -v < ALVO >

4) Verificar Rede de Rogue APs.

nmap -A -p1-85,113,443,8080-8100 -T4 –min-hostgroup 50 –max-rtt-timeout 2000 –initial-rtt-timeout 300 –max-retries 3 –host-timeout 20m –max-scan-delay 1000 -oA wapscan 10.0.0.0/8

Eu usei esta verificação para encontrar com êxito muitos APs em uma rede muito, muito grande.

5) Use um chamariz durante a digitalização de portas para evitar ser pego pelo administrador de sistemas

sudo nmap -sS 192.168.0.10 -D 192.168.0.2

Verificar se há portas abertas no dispositivo de destino do computador (192.168.0.10), enquanto a criação de um endereço de IP (192.168.0.2). Isto irá mostrar o endereço ip falso em vez do seu ip em alvos. Verifique o log de segurança de alvos em /var/log/secure para ter certeza que funcionou.

6) Verifique se há o vírus Conficker na sua LAN ect.

nmap -PN -T4 -p139,445 -n -v –script=smb-check-vulns –script-args safe=1 192.168.0.1-254

substituir 192.168.0.1-256 com o IP que você deseja verificar.

7) Lista de registros de DNS reverso para uma sub-rede

nmap -R -sL 209.85.229.99/27 | awk ‘{if($3==”not”)print”(“$2″) no PTR”;else print$3″ is “$2}’ | grep ‘(‘

Este comando utiliza o nmap para executar consultas de DNS reverso em uma sub-rede. Ela produz uma lista de endereços IP com o correspondente registro PTR para uma determinada sub-rede. Você pode entrar na sub-rede na notação CDIR (i.e. /24 para um Classe C)). Você poderia adicionar “xxxx-dns-servers” após o “-sL ” se você precisar de pesquisas para ser executada em um servidor DNS específico. Em algumas instalações necessidades nmap se executa em sudo. Também espero que awk seja padrão na maioria das distros.

8) Encontre todos os endereços de IP em uma rede

nmap -sP 192.168.0.*

Existem várias outras opções.

Outra opção é:

nmap -sP 192.168.0.0/24

para sub-redes específicas.

9) Como muitas distribuições Linux e Windows, quais dispositivos estão em sua rede?

sudo nmap -F -O 192.168.0.1-255 | grep “Running: ” > /tmp/os; echo “$(cat /tmp/os | grep Linux | wc -l) Linux device(s)”; echo “$(cat /tmp/os | grep Windows | wc -l) Window(s) devices”

10) Encontre IPs não utilizados em uma determinada sub-redes

nmap -T4 -sP 192.168.2.0/24 && egrep “00:00:00:00:00:00″ /proc/net/arp