eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Varreduras Intrusivas**
  - ✓ Conhecendo o Nmap
    - ✓ Principais comandos
    - ✓ Buscando por Serviços
    - ✓ Versões de Serviços ativos
    - ✓ Protocolo TCP
    - ✓ Protocolo UDP
    - ✓ Varredura com SYN Scan
  - ✓ Monitorando Pacotes com Sniffer

Conhecendo o Nmap

Conhecendo o NMAP

Nmap é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker "Fyodor". É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.

É conhecido pela sua rapidez e pelas opções que dispõe.

O Nmap é um programa CUI (Console User Interface), pelo que corre na linha de comandos, mas este tem uma interface gráfica (GUI), o NmapFE (Nmap Front End), que foi substituido pelo Zenmap em 11 de Outubro de 2007, por ser uma versão portátil e prover uma interface melhor para execução e especialmente para visualização e análise dos resultados do Nmap.

Principais comandos

Principais comandos NMAP:

-p

Você pode determinar que uma porta ou sequencia de portas seja varrida, sendo assim, ele não executa a varredura apenas em portas baixas:

Nmap –p 22 192.168.1.1
Nmap –p 22-90 192.168.1.0/24
Nmap –p 22,55,90 192.168.1.1

-g

Define a porta de origem. Como sabemos, geralmente as portas de origem são portas altas (acima de 1024).

Com o Nmap, podemos dizer que a requisição ou o Scan está partindo de uma porta baixa:

Nmap –g 53 192.168.1.1
Nmap –g 22 192.168.1.0/24

Principais comandos

-sP

Ping scan: Algumas vezes é necessário saber se um determinado host ou rede está no ar. Nmap pode enviar pacotes ICMP “echo request” para verificar se determinado host ou rede está ativa. Hoje em dia, existem muitos filtros que rejeitam os pacotes ICMP “echo request”, então envia um pacote TCP ACK para a porta 80 (default) e caso receba RST o alvo está ativo. A terceira técnica envia um pacote SYN e espera um RST ou SYN-ACK.

Nmap –sP 192.168.1.254

Nmap –sP 192.168.1.0/24

-sV

Version detection: Após as portas TCP e/ou UDP serem descobertas por algum dos métodos, o nmap irá determinar qual o serviço está rodando atualmente. O arquivo nmap-service-probes é utilizado para determinar tipos de protocolos, nome da aplicação, número da versão e outros detalhes

Nmap –sV 192.168.1.254

Principais comandos

-sR

RCP scan: Este método trabalha em conjunto com várias técnicas do Nmap. Ele considera todas as portas TCP e UDP abertas e envia comandos NULL SunRPC,para determinar se realmente são portas RPC. É como se o comando "rpcinfo -p" estivesse sendo utilizado, mesmo através de um firewall (ou protegido por TCPwrappers).

Nmap –sR 192.168.1.254

Nmap –sR 192.168.1.0/24

-sS

TCP SYN scan: Técnica também conhecida como "*half-open*", pois não abre uma conexão TCP completa. É enviado um pacote SYN, como se ele fosse uma conexão real e aguarda uma resposta. Caso um pacote SYN-ACK seja recebido, aporta está aberta, enquanto um como resposta indica que a porta está fechada. A vantagem dessa abordagem é que poucos irão detectar esse scanning de portas.

Nmap –sS 192.168.1.254

Nmap –sS 192.168.1.0/24

Principais comandos

-sn

Ping Scan: Durante o Scan, o Nmap verifica o status da porta, porém, com a opção –sn ele verifica apenas se a máquina está viva, sem efetuar scan de portas.

Nmap –sn 192.168.1.254

Nmap –sn 192.168.1.0/24

-sL

List Scan: Com esta opção o Nmap verifica quantos IPs ele irá verificar. Com esta opção ele não varre as máquinas, mas te retorna uma lista de IPs que podem ser varridos em uma determinada rede.

Nmap –sL 192.168.1.0/24

-O

OS detection: É possível descobrir qual o sistema operacional da vítima, ou chegar o mais próximo possível.

Nmap –O 192.168.1.254

Nmap –O 192.168.1.0/24

Principais comandos

--A

Advanced: O Nmap efetua todas as varreduras possíveis para trazer o máximo de informações sobre o alvo, sendo assim, todas as informações possíveis.

Nmap –A 192.168.1.254

Nmap –A 192.168.1.0/24

-n

Nunca Resolver DNS: Ao efetuar a varredura em determinadas máquinas, ele não efetua a resolução de DNS.

Nmap –n 192.168.1.254

Nmap –n 192.168.1.0/24

-R

Sempre resolver DNS: Com esta opção, ele sempre tentará resolver DNS, ou seja, ele sempre tentará descobrir o hostname do alvo baseado em consulta DNS.

Nmap –R 192.168.1.254

Nmap –R 192.168.1.0/24

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker