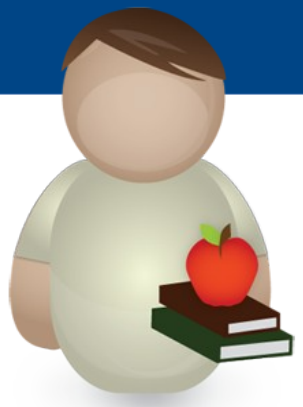

Disciplina:
Segurança de Redes

Professor:
Roitier Campos

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.

NMAP

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;
- Monitoramento de host;
- Disponibilidade de serviço.

Instalação

#apt-get install nmap

Sinopse...

nmap [<Scan Type> ...] [<Options>] { <target specification> }

Onde o (target) é o endereço IP do alvo (host) ou rede que se deseja escanear. Caso exista uma forma de resolver nomes, como um DNS configurado, você pode usar o nome do host ao invés do IP.

Os parâmetros para <Scan Type> são ajustados de acordo com o que se deseja obter, os principais são:

-sT → **C**om esse parâmetro é feito um escaneamento através de tentativas de conexão TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS;

-sS → Assim, a tentativa será com pacotes TCP com a flag SYN ligada, ou seja, como apenas uma requisição de conexão. Essa técnica dificulta um pouco a detecção;

-sP → Com essa opção o escaneamento será feito através de pacotes ICMP echo request. Verifica apenas se o host está ativo;

...Sinopse

-sU → Envia pacotes UDP com 0 byte para determinar o estado dessas portas;

-sO → É usado para tentar determinar os protocolos suportados pelo host;

-O → Com esse parâmetro é feito uma tentativa de determinar o sistema operacional de um host (no sentido de ser atacado).

Com a opção **-p** podemos especificar portas ou faixas (ranges) de portas para análise.

A saída do Nmap é uma lista de alvos escaneados, com informações adicionais de cada um dependendo das opções utilizadas. Essa tabela lista o número da porta e o protocolo, o nome do serviço e o **estado**.

Estado

- **aberto (open)**

Aberto (open) significa que uma aplicação na máquina-alvo está escutando as conexões/pacotes naquela porta.

- **filtrado (filtered)**

Filtrado (filtered) significa que o firewall, filtro ou outro obstáculo de rede está bloqueando a porta de forma que o Nmap não consegue dizer se ela está aberta (open) ou fechada (closed).

- **fechado (closed)**

Portas fechadas (closed)não possuem uma aplicação escutando nelas, embora possam abrir a qualquer instante.

- **não-filtrado (unfilterd)**

Portas são classificadas como não filtradas (unfiltered)quando elas respondem às sondagens do Nmap, mas o Nmap não consegue determinar se as portas estão abertas ou fechadas.

O Nmap reporta as combinações aberta|filtrada (open|filtered)e fechada|filtrada (closed| filtered)quando não consegue determinar qual dos dois estados descrevem melhor a porta.

Alguns detalhes

A tabela de portas também pode incluir detalhes de versão de software quando a detecção de versão for solicitada.

Quando um scan do protocolo IP é solicitado (-sO), o Nmap fornece informações dos protocolos IP suportados ao invés de portas que estejam abertas.

Além da tabela de portas interessantes, o Nmap pode fornecer informações adicionais sobre os alvos, incluindo nomes de DNS reverso, possível sistema operacional, tipos de dispositivos e endereços MAC.

Exemplo

 # nmap -A -T4 “alvo”

-A → para habilitar a detecção de SO e a versão;

-T4 → para execução mais rápida.

Algumas demonstrações

- nmap -sP <ip_do_host> - Verificar se o host está ativo
- nmap <ip_do_host> - Verificar portas abertas
- nmap –p <1000-2000> <ip_do_host> - Verificar range de portas (1000 a 2000)
- nmap –p 22 150.162.65.* - Scanea toda a rede em uma determinada porta --- isso para mascara 255.255.255.0
- nmap –O <ip_do_host_alvo> - Fingerprint de Sistema Operacional
- nmap -sV <ip_do_host_alvo> Fingerprint de um Serviço
- nmap -sS 192.168.0.1 -p 1-100 - testar com pacotes SYN, nas portas de 1 a 100
- nmap -sS 192.168.0.0/24 -p 1-150
- nmap -sT 200.143.14.48 – Testando IP Público (fora da rede), todas as portas

NMAP com Interface

ZENMAP

#apt-get install zenmap

Atividade Complementar

1 - Identifique um endereço da rede local e faça:

(a) Realize a varredura simplesmente (texto e gráfico)

(c) Verifique as portas encontradas abertas e indique o serviço associado.

2 – Supondo que a rede é de sua propriedade, faça um scan na rede local e registre o que observa como resposta.

3 - Tome por base o item 2, mas desta vez, suponha que a rede não é de sua

propriedade e que você deve evitar ao máximo levantar suspeitas de que a rede está sendo varrida. Faça o teste varrendo a rede com a opção –PS, utilizando o comando e registre o que observa como resposta.

Atividade Complementar

4 - Suponha que você queira descobrir os hosts da rede e você sabe que podem existir firewalls bloqueando o caminho. Caso os pacotes do Nmap encontrem um firewall, a resposta pode ser comprometida e não condizente com a realidade. Sabendo disto, você precisa maximizar as chances de obter bons resultados.

Qual o comando que será utilizado?

Teste com o Windows, pois há um firewall que pode ser ativado/desativado.

Registre o que observa como resposta.

Enganando um firewall

O NMAP também pode burlar os firewalls que são configurados para descartar os pedidos de conexões de outras redes. Para isso mudaremos a opção -D, que na verdade vai camuflar seu IP e com isso conseguiremos fazer nossa varredura.

Usando essa opção associada com as outras temos uma das melhores buscas por portas possível. Essa opção será utilizada em conjunto com as outras vindo a frente das demais.

Exemplo:

nmap -sS x.x.x.x **-D** y.y.y.y**,**z.z.z.z

Onde:

x.x.x.x é o IP o qual vou fazer a verificação.

y.y.y.y é o meu IP.

z.z.z.z é um IP qualquer que foi escolhido para que camufle o meu IP.

Proteção contra Scan de Portas

- Firewalls com regras bem definidas;
- Diminuição dos serviços ativos no gateway;
- Análise constante de seus arquivos de log;
- Um IDS, sistema de detecção de intrusos